1 Základní formalismy matematiky

Motivace: *Studium informatiky neznamená jen „naučit se nějaký programovací jazyk“, nýbrž zahrnuje celý soubor dalších relevantních předmětů, mezi nimiž najdeme i matematicko–teoretické (formální) základy moderní informatiky.* □

Náplní prvních dvou lekcí našeho předmětu je právě studenty do potřebných matematických formalismů uvést a dát jim tak první ochutnávku „matematiky vysokoškolské úrovně“. Tato matematika je (možná na rozdíl od vaší dosavadní středoškolské zkušenosti) založena na přesném formálním vyjadřování, chápání a odvozování a na rigorózním úsudku podloženém poctivou matematickou logikou. □

Stručný přehled lekce

* Pochopení přirozeného i formálního zápisu a významu matematických tvrzení (vět).
* Pochopení správného formálního způsobu argumentace v matematice (důkazů).
* Rozbor logické struktury matematických vět a pojem výroku. Základy výrokové logiky.

1.1 Význam matematických tvrzení

Matematika (tudíž i teoretická informatika jako její součást) se vyznačuje velmi přísnými formálními požadavky na korektnost vyjadřování a argumentace.

- Matematické tvrzení je obvykle vysloveno ve tvaru

  „Jestliže platí *předpoklady*, pak platí *závěr*“.

- Tomuto tvaru se odborně říká *implikace*.
- Pro pochopení významu je klíčové vždy správně identifikovat, co jsou v dané větě ony zmíněné předpoklady a co je závěrem.
- Příklady běžné formulace *matematických vět*:
  - ∗ Je-li $x > 1$, pak platí $x^2 > x$.
  - ∗ Konečná množina má konečně mnoho podmnožin.
  - ∗ $\sin^2(\alpha) + \cos^2(\alpha) = 1$.
  - ∗ Graf je rovinný, jestliže neobsahuje podrozdělení K_5 nebo $K_{3,3}$.
- Co přesně nám uvedené matematické věty říkají?

  Často pomůže pouhé rozepsání definic pojmů, které se v dané větě vyskytují.

O pravdivosti implikace

Hned na začátek výkladu zdůrazňujeme, jak moc důležité je pochopit správný logický význam matematického tvrzení vysloveného zmíněnou formou implikace („jestliže . . . , pak . . . “). □

Pravdivost takového tvrzení je třeba chápat v následujícím významu:

Pro každou situaci, ve které jsou splněny všechny předpoklady, (*)
je platný i závěr tvrzení.□

Volně řečeno, z předchozího kritéria (*) vyplývá, že pokud předpoklady nejsou splněny nebo jsou sporné, tak celé tvrzení je platné bez ohledu na pravdivost závěru!

$$\text{NEPRAVDA} \;\Rightarrow\; \text{COKOLIV}$$

Příklad 1.1. *Je pravdivé následující matematické tvrzení?*

> **Věta**. *Mějme dvě kuličky, červenou a modrou. Jestliže červená kulička je těžší než modrá a zároveň je modrá kulička těžší než ta červená, tak jsou obě kuličky ve skutečnosti zelené.* □
>
> *„To přece nemůže být pravda, jak může být jedna kulička těžší než druhá a naopak zároveň? Jak mohou být nakonec obě zelené? To je celé nějaká blbost... “* □

Ano, výše uvedené jsou typické laické reakce na uvedenou větu. Přesto však tato věta pravdivá je!

Stačí se vrátit o kousek výše ke kritériu – Pro každou situaci, ve které jsou splněny všechny předpoklady, je platný i závěr tvrzení – které je zjevně naplněno. Nenaleznete totiž situaci, ve které by byly splněny oba předpoklady zároveň, a tudíž ve všech takových neexistujících situacích si můžete říkat cokoliv, třeba že kuličky jsou zelené. □

Příklad 1.2. *Anna a Klára přišly na přednášku a usadily se do lavic. Proč je pravdivé toto matematické tvrzení?*

> **Věta**. *Jestliže Anna sedí v první řadě lavic a zároveň Anna sedí v poslední řadě lavic, tak Klára nesedí ve druhé řadě lavic.* □

Opět je třeba se pečlivě zamyslet nad významem předpokladů a závěru. Avšak tentokrát není situace předpokladů tak triviálně sporná, jako byla v Příkladu 1.1. Kdy tedy mohou nastat oba předpoklady (o tom, kde sedí Anna) zároveň? □

Když první řada lavic je zároveň řadou poslední. □

Neboli posluchárna má jen (nejvýše) jednu řadu lavic a Klára tudíž v druhé řadě nemůže sedět. Pravdivost celé věty je tímto potvrzena. □

1.2 Úvod do matematického dokazování

S přísnými formálními požadavky na korektnost vyjádření a argumentace v matematice se pojí otázka, jak správně svá tvrzení zdůvodňovat.

Krátce lze říci, že korektně postavená matematická argumentace musí vést od přijatých předpokladů v elementárních krocích směrem k požadovanému závěru (a nikdy ne naopak!). □

- Uvažme matematickou *větu* (neboli tvrzení) tvaru

  „Jestliže platí předpoklady, pak platí závěr“. □

- Důkaz této věty je konečná posloupnost tvrzení, kde
  - ∗ každé tvrzení je buď □
    - – *předpoklad*, nebo
    - – obecně přijatá „pravda“ – *axiom*, nebo
    - – plyne z předchozích a dříve dokázaných tvrzení podle nějakého „akceptovaného“ logického principu – *odvozovacího pravidla*; □
  - ∗ poslední tvrzení je *závěr*.

Příklad 1.4. *Uvažujme následující matematické tvrzení (které jistě už znáte).*

Věta. *Jestliže x je součtem dvou lichých čísel, pak x je sudé.*

Poznámka pro připomenutí:

- *Sudé* číslo je celé číslo dělitelné 2, tj. tvaru $2k$.
- *Liché* číslo je celé číslo nedělitelné 2, tj. tvaru $2k+1$. □

Důkaz postupuje v následujících formálních krocích:

	tvrzení	zdůvodnění
1)	$a = 2k+1$, k celé	předpoklad
2)	$b = 2l+1$, l celé	předpoklad□
3)	$x = a+b = 2k+2l+1+1$	z 1,2) a komutativity sčítání (axiom)□
4)	$x = 2(k+l)+2\cdot 1$	ze 3) a distributivnosti násobení (axiom)□
5)	$x = 2(k+l+1)$	ze 4) a opět distributivnosti násobení□
6)	$x = 2m$, m celé	z 5) a $m = k+l+1$ je celé číslo (axiom)

□

Příklad 1.5. *Dokažte následující tvrzení:*

> **Věta**. *Jestliže x a y jsou racionální čísla pro která platí $x < y$, pak existuje racionální číslo z pro které platí $x < z < y$.* □

Důkaz po krocích (s již trochu méně formálním zápisem) zní:

---

1) Nechť $z = \frac{x+y}{2} = x + \frac{y-x}{2} = y - \frac{y-x}{2}$. □
2) Číslo z je racionální, neboť x a y jsou racionální.
3) Platí $z > x$, neboť $\frac{y-x}{2} > 0$.
4) Dále platí $z < y$, neboť opět $\frac{y-x}{2} > 0$.
5) Celkem $x < z < y$. □

Všimněte si, že klíčový krok (1) popisuje námi vymyšlenou (prostě uhodnutou) algebraickou konstrukci, která vede k požadovanému číslu z. Zbylé kroky (2–5) pak jen snadno zdůvodňují, že nalezené z má všechny požadované vlastnosti. □

1.3 Výroky

- Důležitým pevným mostem mezi běžnou mluvou a přesným matematickým formalismem je pojem výroku. □

Definice 1.6. **Výrok** v přirozené mluvě:
V běžné mluvě za *výrok* považujeme (každé) tvrzení, o kterém má smysl platně prohlásit, že je buď pravdivé, nebo nepravdivé.□

Ukážeme si několik příkladů – které z nich jsou výroky?

* Dnes už v Brně pršelo.□
* Předmět FI: IB000 se vyučuje v prvním ročníku.□
* Platí $2 + 3 = 6$.□
* To je bez problémů. (Co?)□
* Platí $x > 3$.□
* Pro každé celé číslo x platí, že $x > 3$.□

Všimněte si, že pravdivost výroku by mělo být možné rozhodnout bez skrytých souvislostí (kontextu), a proto čtvrtý a pátý příklad za výroky nepovažujeme.

- Z více jednoduchých výroků vytváříme výroky složitější pomocí tzv. *logických spojek*.

Následuje několik dalších příkladů.

* Množina $\{a, b\}$ má více než jeden prvek a není nekonečná. □
* Jestliže Karel váží přes 90 kg, nejedu s ním výtahem. □
* Jestliže má tato kráva 10 nohou, pak mají všechny domy modrou střechu.

Zastavme se na chvíli nad posledním výrokem. Co nám říká? Je pravdivý? □ Skutečně mají všechny domy modrou střechu a před námi stojí kráva s 10 nohama? □

Přirozené vs. formální

- Schopnost porozumět podobným větám je součást lidského způsobu uvažování a z tohoto hlediska nemá přímou souvislost s matematikou (je to „přirozená logika“). □
- *Formální (matematická) logika* pak v podobném duchu definuje jazyk matematiky a přitom odstraňuje nejednoznačnosti přirozeného jazyka.

1.4 Formální výroková logika

Všimněte si, že podle Definice 1.6 každému výroku běžné mluvy lze přiřadit logickou hodnotu 0 (false) nebo 1 (true) a dále se nestarat o jazykový význam…

Proto jazykové výroky v matematice můžeme nahradit *výrokovými proměnnými*, které značíme velkými písmeny $A, B, C, \ldots$ a přiřadíme jim hodnotu 0 nebo 1. □

Definice: *Výroková formule* (značíme $\varphi, \sigma, \psi, \ldots$) vzniká z výrokových proměnných pomocí závorek a logických spojek, □ které z později vysvětlených důvodů dělíme na

* základní spojky $\neg$ *negace* a $\Rightarrow$ *implikace* □
* a odvozené spojky $\vee$ *disjunkce*, $\wedge$ *konjunkce* a $\Leftrightarrow$ *ekvivalence*. □

Při zápise výrokových formulí je potřeba dávat pozor na správné závorkování, aby formule měla jednoznačný význam. Na intuitivní úrovni to ilustrujeme takto:

Správně	A, $(A) \Rightarrow (B)$, $A \Rightarrow B$, $\neg A \Rightarrow B$, $A \vee B \vee \neg C$
a nesprávně	$A \Rightarrow B \Rightarrow C$ – znamená toto $(A \Rightarrow B) \Rightarrow C$ nebo $A \Rightarrow (B \Rightarrow C)$?

Definice 1.8. Sémantika (význam) výrokové logiky.
Nechť *valuace* (ohodnocení) je funkce $\nu : Prom \to \{0,1\}$ na všech (dotčených) výrokových proměnných. Pro každou valuaci ν definujeme funkci $\mathcal{S}_\nu(\sigma)$, *vyhodnocení* formule σ, induktivně (tj. po krocích) takto:

- $\mathcal{S}_\nu(A) := \nu(A)$ pro každé $A \in Prom$.
- $\mathcal{S}_\nu(\neg\varphi) := \begin{cases} 1 & \text{jestliže } \mathcal{S}_\nu(\varphi) = 0; \\ 0 & \text{jinak.} \end{cases}$
- $\mathcal{S}_\nu(\varphi \Rightarrow \psi) := \begin{cases} 0 & \text{jestliže } \mathcal{S}_\nu(\varphi) = 1 \text{ a } \mathcal{S}_\nu(\psi) = 0; \\ 1 & \text{jinak.} \end{cases}$
- $\mathcal{S}_\nu(\varphi \vee \psi) := \mathcal{S}_\nu(\neg\varphi \Rightarrow \psi)$; to jinými slovy znamená

  $\mathcal{S}_\nu(\varphi \vee \psi) = 1$ právě když $\big(\mathcal{S}_\nu(\varphi) = 1$ nebo $\mathcal{S}_\nu(\psi) = 1\big)$.
- $\mathcal{S}_\nu(\varphi \wedge \psi) := \mathcal{S}_\nu(\neg(\neg\varphi \vee \neg\psi))$; to jinými slovy znamená

  $\mathcal{S}_\nu(\varphi \vee \psi) = 1$ právě když $\big(\mathcal{S}_\nu(\varphi) = 1$ a současně $\mathcal{S}_\nu(\psi) = 1\big)$.
- $\mathcal{S}_\nu(\varphi \Leftrightarrow \psi) := \mathcal{S}_\nu((\varphi \Rightarrow \psi) \wedge (\psi \Rightarrow \varphi))$; to jinými slovy znamená

  $\mathcal{S}_\nu(\varphi \Leftrightarrow \psi) = 1$ právě když platí jedna z následujících podmínek
  - $\mathcal{S}_\nu(\varphi) = 1$ a současně $\mathcal{S}_\nu(\psi) = 1$,
  - nebo $\mathcal{S}_\nu(\varphi) = 0$ a současně $\mathcal{S}_\nu(\psi) = 0$.

$\square$

Pravdivostní tabulky

V praxi často vyhodnocení logické výrokové formule zapisujeme do tzv. *pravdivostní tabulky*. Tato tabulka typicky má sloupce pro jednotlivé proměnné, případné „meziformule“ (pomůcka pro snazší vyplnění) a výslednou formuli. Řádků je 2^p (počet valuací), kde p je počet použitých proměnných. □

Příklad 1.9. *Jaká je pravdivostní tabulka pro formuli* $(A \Rightarrow B) \vee B \vee C$?

A	B	C	$A \Rightarrow B$	$(A \Rightarrow B) \vee B \vee C$
0	0	0	1	1
0	0	1	1	1
0	1	0	1	1
0	1	1	1	1
1	0	0	0	0
1	0	1	0	1
1	1	0	1	1
1	1	1	1	1

□

Splnitelnost formulí a tautologie

Definice: Formule φ je *splnitelná*, pokud pro některou valuaci ν platí, že $\mathcal{S}_\nu(\varphi) = 1$. Formule je nesplnitelná (říká se *kontradikce*), pokud není splnitelná. $\square$

Formule φ je vždy pravdivá, neboli výroková *tautologie*, psáno $\models \varphi$, pokud pro každou valuaci ν platí, že $\mathcal{S}_\nu(\varphi) = 1$. $\square$

Řekneme, že dvě formule φ, ψ jsou *ekvivalentní*, právě když $\models \varphi \Leftrightarrow \psi$. $\square$

Tvrzení 1.10. *Následující formule jsou tautologiemi:*

- $\models A \vee \neg A$ $\square$
- $\models \neg\neg A \Leftrightarrow A$ $\square$
- $\models (A \wedge (A \Rightarrow B)) \Rightarrow B$ $\square$
- $\models (\neg B \Rightarrow \neg A) \Rightarrow (A \Rightarrow B)$ $\square$
- $\models (\neg A \Rightarrow (B \wedge \neg B)) \Rightarrow A$

Jak poznáme tautologie v pravdivostní tabulce? A jak ekvivalentní formule?

Ekvivalentní formule pravdivostní tabulkou

Příklad 1.11. *Jsou následující dvě výrokové formule* $(A \Rightarrow B) \wedge \neg(B \vee A)$ *a* $(C \wedge B) \vee (B \wedge \neg C)$ *ekvivalentní?*

Pozor ale při řešení na zkratkovité úvahy ve stylu „přece ty formule mají různé množiny proměnných, tak ekvivalentní být nemůžou“!

Zopakujme si definici ekvivalentních formulí a z ní nahlédneme, že musíme využít pravdivostní tabulku kombinující všechny tři proměnné v našich formulích:

A	B	C	$(A \Rightarrow B) \wedge (B \vee A)$	$(C \wedge B) \vee (B \wedge \neg C)$
0	0	0	0	0
0	0	1	0	0
0	1	0	1	1
0	1	1	1	1
1	0	0	0	0
1	0	1	0	0
1	1	0	1	1
1	1	1	1	1

Ano, dané formule jsou ekvivalentní. □